

# **Exhibit G**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for Content  
and Other Information Associated with  
the Apple iCloud Account with ID  
[REDACTED] and registration email  
[REDACTED]  
Maintained at Premises Controlled by  
Apple Inc., USAO Reference No.  
2020R00816

22 MAG 5801

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Apple Inc. ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

**1. Warrant.** Upon an affidavit of Special Agent Mary Jo Corkery of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the Apple iCloud account with associated [REDACTED] and registration email [REDACTED] (the "Subject Account"), maintained at premises controlled by the Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

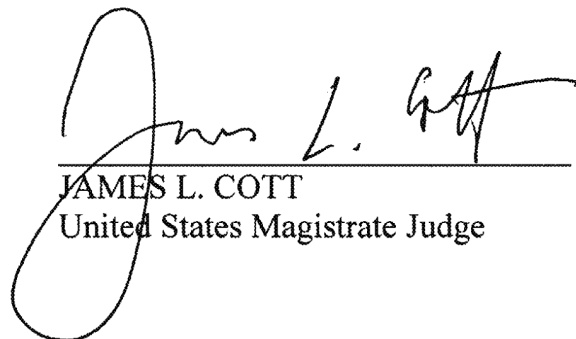
**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, flight from prosecution, and/or intimidation of potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

July 14, 2022  
Date Issued

9:18 a.m.  
Time Issued



JAMES L. COTT  
United States Magistrate Judge

## **Search Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Apple Inc. (the “Provider”), headquartered at 1 Infinite Loop, Cupertino, California 95014, and applies to all content and other information within the Provider’s possession, custody, or control associated with the iCloud account with associated ID [REDACTED] and registration email [REDACTED] (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is directed to produce the following information associated with the Subject Account:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from January 1, 2016 through the date of this Order, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from January 1, 2016 through the date of this Order, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).



### III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of (i) 18 U.S.C. §§ 201 and 371 (bribing or offering to bribe or demanding or accepting a bribe, and conspiring to do the same); (ii) 18 U.S.C. §§ 1343, 1346, and 1349 (wire fraud and honest services wire fraud, and conspiring to commit wire fraud and honest services wire fraud); (iii) 18 U.S.C. § 1951 (extortion under color of right and conspiring to do the same); (iv) 18 U.S.C. §§ 1956 and 1957 (money laundering, engaging in a financial transaction in criminally-derived property, and conspiracy to do one or both of the same); (v) 18 U.S.C. §§ 1001 and 371 (making false statements and conspiring to do the same); and (vi) 18 U.S.C. §§ 1503, 1512 and 371 (obstruction of justice and conspiring to do the same) (collectively, the “Subject Offenses”), including the following:

- Communications between or involving one or more of Nadine Arslanian a/k/a Nadine Menendez (“Arslanian”), Robert Menendez, Wael Hana, Jose Uribe, [REDACTED], Fred Daibes, [REDACTED], [REDACTED], and/or others, or photographs or other documents, reflecting or concerning interactions between Hana, Uribe, [REDACTED], Fred Daibes, [REDACTED] on the one hand, and Menendez or others acting on Menendez’s behalf, on the other hand;

- [REDACTED]

- 

- 

- 

- 

- 

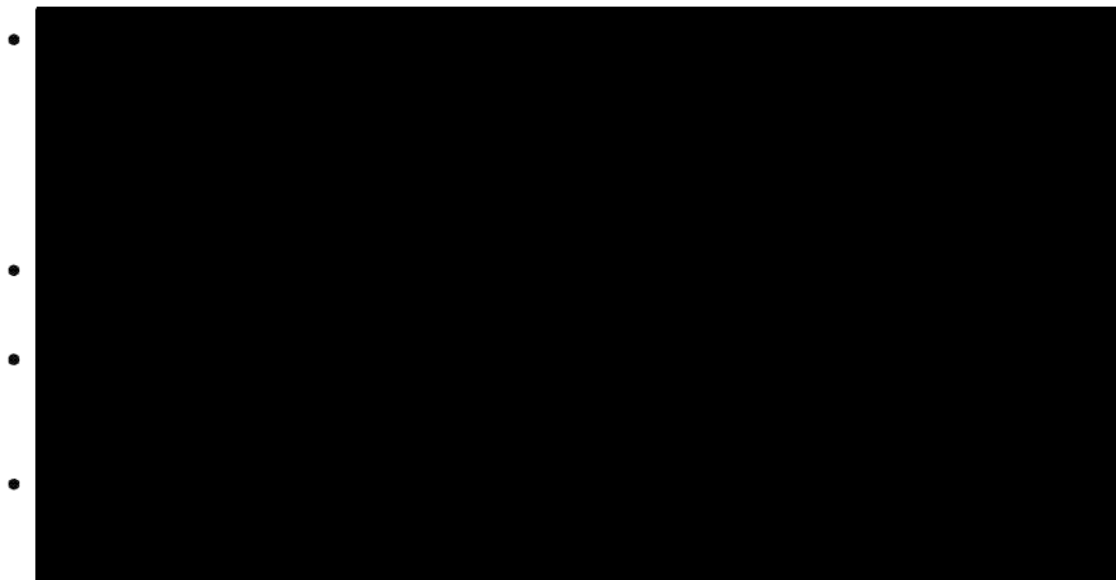
- 

- 

- 

09.20.2021





Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client, Speech or Debate, or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges, and/or production to the account holder’s counsel for initial review and assertion of the Speech or Debate privilege potentially prior to any government review, which initial review shall be reasonably timely, and involve the creation of a privilege log to be shared with the Government, with any dispute subject to oversight by the court.

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for Content  
and Other Information Associated with  
the Email Account

[REDACTED]

Maintained at Premises Controlled by  
Google LLC, USAO Reference No.  
2020R00816

22 MAG 5801

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Google LLC (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

**1. Warrant.** Upon an affidavit of Special Agent Mary Jo Corkery of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account [REDACTED] (the “Subject Account”), maintained at premises controlled by the Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

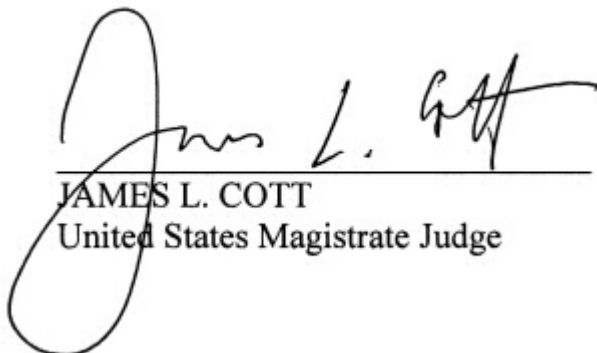
**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, flight from prosecution, and/or intimidation of potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

July 14, 2022  
Date Issued

9:18 a.m.  
Time Issued



JAMES L. COTT  
United States Magistrate Judge

## **Email Search Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Google LLC (the “Provider”), headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, and applies to all content and other information within the Provider’s possession, custody, or control associated with the email account [REDACTED] (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with, the Subject Account(s), including all message content (including all message content or attachments for emails sent in Google’s “confidential” mode), deleted content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the IP addresses of the sender and recipient of the email), as well as all forwarding and fetching accounts related to the Subject Account(s).

b. *Google Services Data.* The files and contents associated with the Subject Account related to the following Google Services: Web & App Activity, Gmail, Google Services, Google Hangouts, Google Drive, Google Calendar, YouTube, Google Play, iGoogle, Google Photos, Google Play Music, Project Fi, Google My Maps, Google Payments

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account(s), including but not limited to name, username, address, telephone number, recovery and alternate email addresses, sign-in phone numbers, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Chrome Browser and web and search history records.* All records relating to Internet search and browsing history, and application usage history, including My Activity, Web & App Activity, device information history, and location history, including Chrome Browser records.

e. *Device Information.* Any information identifying the device or devices used to access the Subject Account(s), including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the Subject Account(s).

f. *Information Regarding Linked Accounts, Including Accounts Linked by Cookie.* Any information identifying accounts that are associated with or connected to the Subject

Account(s), including but not limited to specifically by cookies; recovery, secondary, forwarding, or alternate email address; Google ID; Android ID; IMEI; creation IP address; telephone number, including SMS recovery number or sign-in account number; or any other account or device identifier.

g. *Transactional records.* All transactional records associated with the Subject Account(s), including any IP logs or other records of session times and durations, along with device information (including user agent strings) used to access the Subject Account(s).

h. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account(s), including complaints, inquiries, or other contacts with support services and records of actions taken.

i. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued by the Government pursuant to 18 U.S.C. § 2703(f), or otherwise.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of (i) 18 U.S.C. §§ 201 and 371 (bribing or offering to bribe or demanding or accepting a bribe, and conspiring to do the same); (ii) 18 U.S.C. §§ 1343, 1346, and 1349 (wire fraud and honest services wire fraud, and conspiring to commit wire fraud and honest services wire fraud); (iii) 18 U.S.C. § 1951 (extortion under color of right and conspiring to do the same); (iv) 18 U.S.C. §§ 1956 and 1957 (money laundering, engaging in a financial transaction in criminally-

derived property, and conspiracy to do one or both of the same); (v) 18 U.S.C. §§ 1001 and 371 (making false statements and conspiring to do the same); and (vi) 18 U.S.C. §§ 1503, 1512 and 371 (obstruction of justice and conspiring to do the same) (collectively, the “Subject Offenses”), including the following:

- Communications between or involving one or more of Nadine Arslanian a/k/a Nadine Menendez (“Arslanian”), Robert Menendez, Wael Hana, Jose Uribe, [REDACTED], Fred Daibes, [REDACTED] and/or others, or photographs or other documents, reflecting or concerning interactions between Hana, Uribe, [REDACTED], Fred Daibes, [REDACTED] on the one hand, and Menendez or others acting on Menendez’s behalf, on the other hand;

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]



- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect

any attorney-client, Speech or Debate, or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges, and/or production to the account holder’s counsel for initial review and assertion of the Speech or Debate privilege potentially prior to any government review, which initial review shall be reasonably timely, and involve the creation of a privilege log to be shared with the Government, with any dispute subject to oversight by the court.